

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023717 A2

(51) International Patent Classification⁷:
9/28, H04N 7/167, H04K 1/00

H04L 9/32,

(74) Agents: KANANEN, Ronald, P. et al.; RADER FISH-
MAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501,
Washington, DC 20036 (US).

(21) International Application Number:

PCT/US2003/027774

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE,
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR,
KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,
MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,
RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR,
TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date:

8 September 2003 (08.09.2003)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

60/409,675

9 September 2002 (09.09.2002)

US

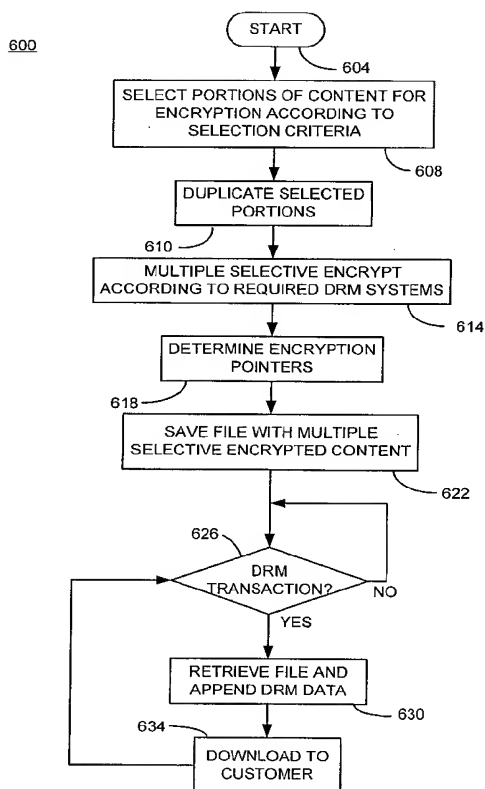
(71) Applicant: SONY ELECTRONICS INC. [US/US]; 1
Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventor: CANDELORE, Brant, L.; 10124 Quail Glen
Way, Escondido, CA 92029-6502 (US).

(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: CONTENT DISTRIBUTION FOR MULTIPLE DIGITAL RIGHTS MANAGEMENT



(57) Abstract: A method and apparatus for enabling use of multiple digital rights management scenarios (DRM). Unencrypted data representing digital content is examined to identify at least segments of content for encryption. The identified segments of content are duplicated and then encrypted using a first encryption method associated with a first DRM to produce first encrypted segments. Duplicates are encrypted using a second encryption method associated with a second DRM to produce second encrypted segments. A set of pointers are generated that point to the first and second encrypted segments content. A file is then created containing first and second encrypted segments of content, pointers and unencrypted content along with DRM rights data to produce a selectively encrypted multiple DRM enabled file.



Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTENT DISTRIBUTION FOR MULTIPLE DIGITAL RIGHTS MANAGEMENT

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to U.S. patent applications serial number 10/273,905, filed October 18, 2002 to Candelore et al. entitled "Video Slice and Active Region Based Dual Partial Encryption", serial number 10/273,903, filed October 18, 2002 to Candelore et al. entitled "Star Pattern Partial Encryption", serial number 10/274,084, filed October 18, 2002 to Candelore et al. entitled "Slice Mask and Moat Pattern Partial Encryption", and serial number 10/274,019, filed October 18, 2002 to Candelore et al. entitled "Video Scene Change Detection", which are hereby incorporated by reference.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/409,675, filed September 9, 2002, entitled "Generic PID Remapping for Content Replacement", to Candelore. This application is also hereby incorporated by reference herein.

1 **COPYRIGHT NOTICE**

2 A portion of the disclosure of this patent document contains material which
3 is subject to copyright protection. The copyright owner has no objection to the
4 facsimile reproduction of the patent document or the patent disclosure, as it
5 appears in the Patent and Trademark Office patent file or records, but otherwise
6 reserves all copyright rights whatsoever.

7

8 **FIELD OF THE INVENTION**

9 This invention relates generally to the field of digital rights management.
10 More particularly, this invention relates to a multiple encryption method and
11 apparatus particularly useful for multiple encrypting digitized video for purposes
12 of enabling multiple digital rights management scenarios (DRMs).

13

14 **BACKGROUND OF THE INVENTION**

15 In traditional distribution of audio and/or video content such as music and
16 movies, rights to copyrighted works are managed by the ownership of the
17 physical medium containing the work. Ownership of the medium provides a
18 limited barrier to unauthorized use. While piracy was and is prevalent with such
19 traditional "packaged media", the problems are dramatically multiplied in an
20 environment of digital distribution of content. The owners of the content have
21 devised various ways to help protect such content that have been collectively
22 termed digital rights management (DRM). DRM encompasses not only the
23 numerous encryption schemes that have been employed to protect the content,
24 but also encompasses the various arrangements for permitting use of the content
25 that have been created, as well as the monitoring and tracking of the rights to the
26 content.

27 Several forms of DRM are currently in place in the marketplace. Perhaps
28 the most dominant DRM forms a part of the Microsoft Windows® operating
29 system's Media Player, and is referred to as "Reciprocal". Another widely used

1 DRM arrangement is built into the Real Networks' Real Player®. Currently the
2 DRM solutions from Microsoft is tightly coupled with the compression algorithm.
3 DRM solutions usually execute on personal computer (PC) platforms.
4 Consequently, the DRM solutions are designed to detect software tampering,
5 and thus efforts are made to obfuscate the operation of the executing software.

6 The above two examples of DRM are but two of an ever growing and
7 evolving field of technology. Further DRM incarnations can be anticipated on a
8 continuing basis to provide greater protection for the content against those who
9 would illegally pirate the content.

10 Unfortunately, due to the multiple types of DRM that are available,
11 customers may have to either acquire multiple sets of software (or plug-ins) that
12 support the various DRM scenarios, or limit consumption of content to those
13 DRMs which they wish to support on their computer.

14

15 BRIEF DESCRIPTION OF THE DRAWINGS

16 The features of the invention believed to be novel are set forth with
17 particularity in the appended claims. The invention itself however, both as to
18 organization and method of operation, together with objects and advantages
19 thereof, may be best understood by reference to the following detailed
20 description of the invention, which describes certain exemplary embodiments of
21 the invention, taken in conjunction with the accompanying drawings in which:

22 **FIGURE 1** is a block diagram of an digital content distribution system
23 including digital rights management consistent with certain embodiments of the
24 present invention.

25 **FIGURE 2** illustrates an exemplary file structure consistent with certain
26 embodiments of the present invention.

27 **FIGURE 3** illustrates a byte offset arrangement for video data consistent
28 with certain embodiments of the present invention.

1 **FIGURE 4** illustrates a byte offset arrangement for audio data consistent
2 with certain embodiments of the present invention.

3 **FIGURE 5** illustrates an exemplary DRM arrangement within video or
4 audio data content consistent with certain embodiments of the present invention.

5 **FIGURE 6** is a flow chart showing a method for encoding content with
6 multiple DRMs consistent with certain embodiments of the present invention.

7 **FIGURE 7** is a flow chart depicting acquisition and playback of content
8 having multiple DRMs consistent with certain embodiments of the present
9 invention.

10 **FIGURE 8** illustrates a content provider server system consistent with
11 certain embodiments of the present invention.

12 **FIGURE 9** is a block diagram of a playback computer consistent with
13 embodiments of the present invention.

14

15 **DETAILED DESCRIPTION OF THE INVENTION**

16 While this invention is susceptible of embodiment in many different forms,
17 there is shown in the drawings and will herein be described in detail specific
18 embodiments, with the understanding that the present disclosure is to be
19 considered as an example of the principles of the invention and not intended to
20 limit the invention to the specific embodiments shown and described. In the
21 description below, like reference numerals are used to describe the same, similar
22 or corresponding parts in the several views of the drawings.

23 The terms "scramble" and "encrypt" and variations thereof are used
24 synonymously herein. The term "video" is often used herein to embrace not only
25 true visual information, but also in the conversational sense (e.g., "video tape
26 recorder") to embrace not only video signals but associated audio and data. The
27 present document generally uses the example of a "dual selective encryption"
28 embodiment, but those skilled in the art will recognize that the present invention
29 can be utilized to realize multiple partial encryption without departing from the

1 invention. The terms "partial encryption" and "selective encryption" are used
2 synonymously herein.

3 The above-referenced commonly owned patent applications describe
4 inventions relating to various aspects of methods generally referred to herein as
5 partial encryption or selective encryption. More particularly, systems are
6 described wherein selected portions of a particular selection of digital content
7 are encrypted using two (or more) encryption techniques while other portions of
8 the content are left unencrypted. By properly selecting the portions to be
9 encrypted, the content can effectively be encrypted for use under multiple
10 decryption systems without the necessity of encryption of the entire selection of
11 content. In some embodiments, only a few percent of data overhead is needed
12 to effectively encrypt the content using multiple encryption systems. This results
13 in a cable or satellite system being able to utilize Set-top boxes or other
14 implementations of conditional access (CA) receivers from multiple
15 manufacturers in a single system - thus freeing the cable or satellite company to
16 competitively shop for providers of Set-top boxes.

17 The present invention applies similar selective encryption techniques to
18 the problem of multiple digital rights management. The partial encryption
19 processes described in the above patent applications utilize any suitable
20 encryption method. However, these encryption techniques are selectively
21 applied to the data stream, rather than encrypting the entire data stream, using
22 techniques described in the above-referenced patent applications. In general,
23 but without the intent to be limiting, the selective encryption process utilizes
24 intelligent selection of information to encrypt so that the entire program does not
25 have to undergo dual encryption. By appropriate selection of data to encrypt, the
26 program material can be effectively scrambled and hidden from those who desire
27 to hack into the system and illegally recover commercial content without paying.
28 MPEG (or similar format) data that are used to represent the audio and video
29 data does so using a high degree of reliance on the redundancy of information

1 from frame to frame. Certain data can be transmitted as "anchor" data
2 representing chrominance and luminance data. That data is then often simply
3 moved about the screen to generate subsequent frames by sending motion
4 vectors that describe the movement of the block. Changes in the chrominance
5 and luminance data are also encoded as changes rather than a recoding of
6 absolute anchor data. Thus, encryption of this anchor data, for example, or other
7 key data can effectively render the video un-viewable.

8 Certain embodiments of the present invention enable a second (or
9 multiple) Digital Rights Management (DRM) solution by duplicating and
10 encrypting content important or critical for decoding the rest of the content with
11 the first and second DRMs. The duplication of content need not add a major
12 increase bandwidth overhead. Unlike terrestrial and satellite broadcast streams,
13 content delivered and eventually decrypted by a PC over the internet does not
14 have to be restricted to 188 byte packets. For terrestrial and satellite streams,
15 hardware decryption is usually performed on per packet basis based on the
16 scrambling bits in the transport header. Content decryption done in software can
17 be much more granular and selective.

18 In accordance with certain embodiments consistent with the present
19 invention, the selected video data to be encrypted may be any individual one or
20 combination of the following (described in greater detail in the above
21 applications): video slice headers appearing in an active region of a video frame,
22 data representing an active region of a video frame, data in a star pattern within
23 the video frame, data representing scene changes, I Frame packets, packets
24 containing motion vectors in a first P frame following an I Frame, packets having
25 an intra_slice_flag indicator set, packets having an intra_slice indicator set,
26 packets containing an intra_coded macroblock, data for a slice containing an
27 intra_coded macroblock, data from a first macroblock following the video slice
28 header, packets containing video slice headers, anchor data, and P Frame data
29 for progressively refreshed video data, data arranged in vertical and or horizontal

1 moat patterns on the video frame, and any other selected data that renders the
2 video and/or audio difficult to utilize. Several such techniques as well as others
3 are disclosed in the above-referenced patent applications, any of which (or other
4 techniques) can be utilized with the present invention to encrypt only a portion of
5 the content.

6 Referring now to **FIGURE 1**, a content delivery system 100 consistent with
7 certain embodiments of the present invention is illustrated. In this system, a
8 digital content provider 104 provides content such as audio or video content to a
9 customer over the Internet for delivery to the customer's personal computer
10 system 112, e.g., by downloading or streaming. Computer system 112 may, for
11 example, be a multimedia computer system having a video display 116 and a
12 stereo (or other multi-channel) audio system that drives a set of speakers such
13 as speakers 120L and 120R. The personal computer 112 operates using any
14 suitable operating system and incorporates one or more software programs for
15 playback of the audio and/or video content (hereinafter, a "media player").

16 The digital content provider may operate as an addressable web site that
17 serves as an online distributor of content. In this example, the web site is shown
18 to have a content database 130 that stores content which can be purchased
19 under various terms by customers having computers such as 112 connected to
20 the Internet. To provide a simplified example, without intent to limit the scope of
21 the present invention, digital content provider 104 is depicted as having the ability
22 to supply content using two digital rights management systems - DRM A shown
23 as 134 and DRM B shown as 138. In a conventional digital content provider
24 scenario, only a single DRM system is used and content is stored in encrypted
25 form using the encryption scenario for that particular DRM system.

26 In accordance with certain embodiments consistent with the present
27 invention, content stored in the content database 130 is stored with dual (in
28 general multiple) selective encryption consistent with the content provider's dual
29 (multiple) DRMs. In this manner, the digital content provider 104 is not burdened

1 with the requirement and cost associated with storage of the content separately
2 under multiple DRMs. Nor is the computing power required to dynamically
3 encrypt the content using a specified DRM at the time of purchase.

4 Content can be arranged for delivery to the customer as a file similar to
5 that depicted in **FIGURE 2**. In this file structure, the file delivered to the customer
6 is stored with selected portions multiply encrypted. In one example, not intended
7 to be limiting, if the content is stored as MPEG data, one can encrypt all of the
8 MPEG I frames or video slice headers to achieve a substantial level of encryption
9 without need to encrypt the entire file. Any other suitable selective encryption
10 arrangement can also be used without limitation. Once a selected portion of the
11 audio and/or video is selected for encryption, the selected portions are duplicated
12 and encrypted. In this example, the selected portions are encrypted under an
13 encryption arrangement consistent with DRM A in one case and consistent with
14 DRM B in the other. The content is then reassembled with the duplicated
15 encrypted content replacing the original clear content. (Note that in other
16 scenarios, content can be stored encrypted or unencrypted and the file
17 processed and constructed for delivery to the customer "on the fly".)

18 In this example of Audio/Video content, the content is stored as audio
19 content 206 and video content 210. The file further contains a set of audio
20 encryption pointers 212 that point to the selected portions of the audio content
21 that are encrypted. Similarly, the file further contains a set of video encryption
22 pointers 218 that point to the selected portions of the video content that are
23 encrypted. DRM A data section 222 provides data that the decoder will need to
24 decode the content encrypted using the encryption scheme of DRM A. Similarly,
25 DRM B data section 226 provides data that the decoder will need to decode the
26 content encrypted using the encryption scheme of DRM B. An identification
27 section 230 identifies the content and the DRM schemes available in the file.

28 The relationship between the video data 210 and video encryption
29 pointers 218 is illustrated in **FIGURE 3**. Pointers are stored that point to

1 encrypted portions of the video data in the file. Such encrypted portions are
2 shown as 304, 308 and 312. Such encrypted portions are interspersed with
3 portions of data stored unencrypted (In the clear) shown as 320, 324, 328 and
4 332. Of course this illustration is quite simplified since only a small number of
5 encrypted segments are shown compared to the likely large number of encrypted
6 segments. In this illustration, each encrypted segment is illustrated to be the
7 same size (i.e., the encryption quanta), but this is not to be interpreted as limiting.

8 The relationship between the audio data 206 and audio encryption
9 pointers 212 is similar and illustrated in **FIGURE 4**. Pointers are stored that point
10 to encrypted portions of the audio data in the file. Such encrypted portions are
11 shown as 404, 408 and 412. Such encrypted portions are interspersed with
12 portions of data stored unencrypted shown as 420, 424, 428 and 432. Again,
13 this illustration is quite simplified since only a small number of encrypted
14 segments are shown compared to the likely large number of encrypted
15 segments. In this illustration, the encrypted segments are shown as differing in
16 size, which can be achieved by specifying the length of each encrypted segment.

17 In each case, the number of bytes to be encrypted can be predefined if
18 desired as the encryption quanta so that the encryption pointers can be simply a
19 sequence of memory offset locations. The amount of data encrypted is then
20 determined by a preset encryption quanta (e.g., 8 bytes). In other embodiments,
21 the encryption pointer section can include not only a starting offset but also an
22 ending offset or a starting offset and a number of bytes.

23 **FIGURE 5** depicts an exemplary section of encrypted content with the
24 byte offset location illustrated at the beginning of the section of encrypted
25 content. The next segment of data is DRM A encrypted content 502 that lasts for
26 a duration determined by the encryption quanta (either predefined or encoded in
27 the encryption pointers). The next segment of encrypted content 506 is
28 encrypted under DMA B's encryption scheme and lasts for a duration again
29 defined by the encryption quanta. By using a predefined encryption quanta, the

1 encryption pointers are simplified. By specifying the size of the encrypted
2 segment, the size can be varied to achieve a more flexible encryption scheme, at
3 the sacrifice of efficiency in the encryption pointers. Note that in the case of a
4 predefined encryption quanta, multiple consecutive segments can be encrypted
5 to achieve the effect of longer segments of encrypted content.

6 DRMs typically verify that the consumer has paid for viewing the content.
7 Viewing may be granted for a period of time or on a viewing event. When a
8 customer makes a payment, this act enables decryption of the content, often as a
9 result of delivery of a decryption key to the customer to enable decryption. In
10 order to enable two or more DRMs to work side-by-side, there should be a clear
11 separation between the payment and key management operation and the
12 content decryption. The media player should allow selection of either DRM. By
13 use of selective encryption, most of the content can be sent in the clear with only
14 certain critical or important content (needed to decompress the rest of the
15 content) sent encrypted. The critical or important content is duplicated and one
16 set of the content is encrypted under one DRM, while the other, is encrypted
17 under the other DRM.

18 Movies and music delivered over the Internet can be packetized in UDP
19 packets for delivery over IP networks. Once re-assembled in the PC, the file can
20 be essentially flat. Both the video and audio can be large packetized elementary
21 stream (PES) files.

22 In order to realize certain embodiments of the present invention, there
23 should be agreement as to how a media player identifies content that is
24 encrypted. In certain embodiments, the encryption quanta, if utilized, should be
25 standardized, or there should be agreement on the least common denominator.
26 Granularity of encryption should be standardized (e.g., can bits from different
27 parts of a video and audio frame be collated for encryption? This is more
28 complicated to signal unless the same bits are chosen over-and-over.). These
29 matters, however, are more properly the subject of standardization negotiations

1 and are not important to the understanding of the concepts and principles
2 governing the present invention.

3 The files described above can be created using any of a number of
4 processes. Moreover, the file structure shown, although illustrated for
5 audio/video content, can be readily adapted to audio only by omission of the
6 video encryption pointers and video content. One process for creation of such
7 files is depicted in **FIGURE 6** as process 600 starting at 604. At 608, a selection
8 criterion is employed to select segments of content to be multiple selectively
9 encrypted. The selection criterion used can be any of those described above,
10 described in the above-referenced patent applications, described elsewhere or
11 newly created without limitation. Once the segments of content are selected,
12 they are duplicated as many times as there are DRM systems to be employed at
13 610. For example, in the digital content provider 104, one set of duplicate
14 selected data is created.

15 The selected content is then multiple encrypted such that each of the
16 duplicate sets of selected data is encrypted under the encryption scheme for
17 each of the DRMs at 614. In the example of content provider 104, the selected
18 segments of content are duplicated. One set of selected segments is encrypted
19 under DRM A and the duplicate set is encrypted under DRM B. A set of
20 encryption pointers is then created at 618 as offset values and possibly
21 information that determines the size of the encrypted portions and the file can be
22 saved in the content database 130 at this point until a customer wishes to
23 acquire digital rights to the content. Alternatively, content can be stored in the
24 clear (or encrypted) and the file for delivery to the customer can be created after
25 purchase by the customer.

26 When a customer purchases rights to the content, a digital rights managed
27 transaction is carried out at 626 in which the customer pays for certain rights.
28 Such rights might include rights to view for a particular time period or number of
29 viewings. Limitations can be imposed on copying, playback machine or other

1 attributes of the DRM during this transaction. When the transaction is complete,
2 the file containing the purchased content is then retrieved from the content
3 database and DRM data defining the purchased rights is appended at 630. The
4 file is then downloaded or streamed to the customer at 634. The customer can
5 then play back the content (either on computer 112 or another playback device)
6 in a manner consistent with the DRM rights acquired in the transaction at 626.

7 Thus, a method of enabling use of multiple digital rights management
8 scenarios (DRM), consistent with certain embodiments of the present invention
9 involves examining unencrypted data representing digital content to identify at
10 least segments of content for encryption; encrypting the identified segments of
11 content using a first encryption method associated with a first DRM to produce
12 first encrypted segments; encrypting the identified segments of content using a
13 second encryption method associated with a second DRM to produce second
14 encrypted segments; generating first pointers to the first encrypted content;
15 generating second pointers to the second encrypted content; and replacing the
16 identified segments of content with the first encrypted content and the second
17 encrypted content in the digital content, and inserting the first and second
18 pointers to produce a partially encrypted dual DRM enabled file. When digital
19 rights are purchased, DRM data enabling the rights are appended to the file and
20 the file is sent to the customer.

21 A process such as that used by the customer in accordance with certain
22 embodiments consistent with the present invention is illustrated as process 700
23 of **FIGURE 7** starting at 702 after which the customer acquires digital rights in
24 content via a digital rights acquisition transaction at 706. The customer can then
25 receive by download or streaming the multiple DRM file at 710. When the
26 customer wishes to initiate playback at 714, the DRM data are read at 718, so
27 that the software on the customer's computer or other playback device can
28 determine if the digital rights acquired by the customer are valid (i.e., not expired
29 or otherwise exhausted). If the software determines that the digital rights have

1 expired or been exhausted at 722, the playback is aborted at 726 and the
2 process ends at 730.

3 If the customer's digital rights are verified at 722, the software reads the
4 file's encryption pointers at 734 and begins reading the content at 738. If the
5 content is encrypted at 742, it is decrypted at 746 according to the selected DRM
6 scheme being used for playback (dependent upon the playback software and/or
7 playback machine). If the content is unencrypted or decrypted, control passes to
8 750 where the content is played or buffered for play. If the end of the file has not
9 been reached at 754, control passes back to 738 where a next segment of
10 content is read. When the end of the file is reached at 754, the process stops at
11 730.

12 Thus, in accordance with certain embodiments consistent with the present
13 invention, a method of using rights to digital content under one of a plurality of
14 digital rights management scenarios (DRM), involves carrying out a transaction
15 to acquire digital rights to the content; receiving digital content containing:
16 segments of unencrypted content, first encrypted segments of content encrypted
17 using a first encryption method associated with a first DRM, second encrypted
18 segments of content encrypted using a second encryption method associated
19 with a second DRM, first pointers to the first encrypted segments of content;
20 second pointers to the second encrypted segments of content, and DRM data
21 that enables digital rights under at least one of the first DRM and the second
22 DRM; determining that valid digital rights are available from the DRM data; and
23 decrypting one of the first and second encrypted segments to enable playing of
24 the content.

25 The process 600 of **FIGURE 6** can be carried out on any suitable
26 programmed general purpose processor operating as a multiple DRM encoder
27 such as that depicted as computer 800 of **FIGURE 8**. Computer 800 has one or
28 more central processor units (CPU) 810 with one or more associated buses 814
29 used to connect the central processor unit 810 to Random Access Memory 818

1 and Non-Volatile Memory 822 in a known manner. Output devices 826, such as
2 a display and printer, are provided in order to display and/or print output for the
3 use of the digital content provider as well as to provide a user interface such as a
4 Graphical User Interface (GUI). Similarly, input devices such as keyboard,
5 mouse and removable media readers 830 may be provided for the input of
6 information by the operator. Computer 800 also incorporates internal and/or
7 external attached disc or other mass storage 834 for storing large amounts of
8 information including, but not limited to, the operating system, multiple DRM
9 encryption methods, as well as the content (which is most likely stored on
10 massive attached storage). The Computer system 800 also has an interface
11 838 for connection to the Internet to service customer requests for content.
12 While depicted as a single computer, the digital content provider may utilize
13 multiple linked computers to carry out the functions described herein.

14 The process 700 of **FIGURE 7** can be carried out on any suitable
15 programmed general purpose processor operating as a decoder/decrypter and
16 DRM validator such as that depicted as computer 900 of **FIGURE 9**. Computer
17 900 may be typical of personal computer devices and has a central processor
18 unit (CPU) 910 with one or more associated buses 914 used to connect the
19 central processor unit 910 to Random Access Memory 918 and Non-Volatile
20 Memory 922 in a known manner. Output devices 926, such as a display adapter
21 and display, are provided in order to display output for the use of the customer
22 (possibly including playback of video content) as well as to provide a user
23 interface such as a Graphical User Interface (GUI). An audio adapter and audio
24 system 928 may also be attached for playback of audio or audio/video content.
25 Similarly, input devices such as keyboard, mouse and removable media readers
26 930 may be provided for the input of information by the operator. Computer 900
27 also incorporates internal and/or external attached disc or other mass storage
28 934 for storing large amounts of information including, but not limited to, the
29 operating system, DRM validation and decryption software, media player

1 software as well as the downloaded content. The Computer system 900 also
2 has an interface 938 for connection to the Internet, e.g. to purchase content.

3 Thus, certain embodiments of the present invention provide for a digital
4 content provider to readily supply content under multiple digital rights
5 management schemes without need to fully encrypt the content for each potential
6 DRM system. This permits a reduction in either storage capacity (for storage or
7 multiple fully encrypted copies of content) or processing power (to encrypt on the
8 fly) needed by the digital content provider. By use of embodiments of the present
9 invention, the customer can be afforded a wide range of content without need to
10 purchase or load multiple DRM systems and media players on his or her
11 personal computer since multiple DRMs can be readily accommodated by the
12 content provider at low cost.

13 Those skilled in the art will recognize that the present invention has been
14 described in terms of exemplary embodiments based upon use of a programmed
15 processor (e.g., computers 800 and 900). However, the invention should not be
16 so limited, since the present invention could be implemented using hardware
17 component equivalents such as special purpose hardware and/or dedicated
18 processors which are equivalents to the invention as described and claimed.
19 Similarly, general purpose computers, microprocessor based computers, micro-
20 controllers, optical computers, analog computers, dedicated processors and/or
21 dedicated hard wired logic may be used to construct alternative equivalent
22 embodiments of the present invention. Moreover, although the present invention
23 has been described in terms of a general purpose personal computer providing a
24 playback mechanism, the playback can be carried on a dedicated machine
25 without departing from the present invention.

26 Those skilled in the art will appreciate that the program steps and
27 associated data used to implement the embodiments described above can be
28 implemented using disc storage as well as other forms of storage such as for
29 example Read Only Memory (ROM) devices, Random Access Memory (RAM)

1 devices; optical storage elements, magnetic storage elements, magneto-optical
2 storage elements, flash memory, core memory and/or other equivalent storage
3 technologies without departing from the present invention. Such alternative
4 storage devices should be considered equivalents.

5 The present invention, as described in embodiments herein, is
6 implemented using a programmed processor executing programming instructions
7 that are broadly described above form that can be stored on any suitable
8 electronic storage medium or transmitted over any suitable electronic
9 communication medium or otherwise be present in any computer readable or
10 propagation medium. However, those skilled in the art will appreciate that the
11 processes described above can be implemented in any number of variations and
12 in many suitable programming languages without departing from the present
13 invention. For example, the order of certain operations carried out can often be
14 varied, additional operations can be added or operations can be deleted without
15 departing from the invention. Error trapping can be added and/or enhanced and
16 variations can be made in user interface and information presentation without
17 departing from the present invention. Such variations are contemplated and
18 considered equivalent.

19 Software code and/or data embodying certain aspects of the present
20 invention may be present in any computer readable medium, transmission
21 medium, storage medium or propagation medium including, but not limited to,
22 electronic storage devices such as those described above, as well as carrier
23 waves, electronic signals, data structures (e.g., trees, linked lists, tables, packets,
24 frames, etc.) optical signals, propagated signals, broadcast signals, transmission
25 media (e.g., circuit connection, cable, twisted pair, fiber optic cables,
26 waveguides, antennas, etc.) and other media that stores, carries or passes the
27 code and/or data. Such media may either store the software code and/or data or
28 serve to transport the code and/or data from one location to another. In the
29 present exemplary embodiments, MPEG compliant packets, slices, tables and

1 other data structures are used, but this should not be considered limiting since
2 other data structures can similarly be used without departing from the present
3 invention.

4 While the invention has been described in conjunction with specific
5 embodiments, it is evident that many alternatives, modifications, permutations
6 and variations will become apparent to those skilled in the art in light of the
7 foregoing description. Accordingly, it is intended that the present invention
8 embrace all such alternatives, modifications and variations as fall within the
9 scope of the appended claims.

1 What is claimed is:

2

3 1. A method of enabling use of multiple digital rights management scenarios
4 (DRM), comprising:

5 examining unencrypted data representing digital content to identify at least
6 segments of content for encryption;

7 encrypting the identified segments of content using a first encryption
8 method associated with a first DRM to produce first encrypted segments;

9 encrypting the identified segments of content using a second encryption
10 method associated with a second DRM to produce second encrypted segments;

11 generating first pointers to the first encrypted segments of content;

12 generating second pointers to the second encrypted segments of content;

13 and

14 replacing the identified segments of content with the first encrypted
15 content and the second encrypted content in the digital content, and inserting the
16 first and second pointers to produce a partially encrypted dual DRM enabled file.

17

18 2. The method according to claim 1, wherein the content comprises digitized
19 audio.

20

21 3. The method according to claim 1, wherein the content comprises digitized
22 video.

23

24 4. The method according to claim 1, further comprising appending data to
25 enable digital rights under the first DRM to the file.

26

27 5. The method according to claim 1, further comprising appending data to
28 enable digital rights under the second DRM to the file.

29

1 6. The method according to claim 1, wherein the first and second pointers
2 comprise byte offsets identifying a starting location for encrypted segments of
3 content.

4

5 7. The method according to claim 1, wherein the first and second encrypted
6 segments of content have a duration defined by an encryption quanta.

7

8 8. The method according to claim 1, further comprising appending data to
9 enable digital rights under at least one of the first DRM and the second DRM to
10 the file; and transmitting the file to a customer.

11

12 9. A computer readable medium storing instructions which, when executed
13 on a programmed processor, carry out the method of method of enabling use of
14 multiple digital rights management scenarios according to claim 1.

15

16 10. An encoder that enables use of multiple digital rights management
17 scenarios (DRM), comprising:

18 means for examining unencrypted data representing digital content to
19 identify at least segments of content for encryption;

20 a first encrypter that encrypts the identified segments of content using a
21 first encryption method associated with a first DRM to produce first encrypted
22 segments;

23 a second encrypter that encrypts the identified segments of content using
24 a second encryption method associated with a second DRM to produce second
25 encrypted segments;

26 means for generating first pointers to the first encrypted segments of
27 content;

28 means for generating second pointers to the second encrypted segments
29 of content; and

1 means for replacing the identified segments of content with the first
2 encrypted content and the second encrypted content in the digital content, and
3 inserting the first and second pointers to produce a partially encrypted dual DRM
4 enabled file.

5

6 11. The encoder according to claim 10, wherein the content comprises at least
7 one of digitized audio and digitized video.

8

9 12. The encoder according to claim 10, further comprising means for
10 appending data to enable digital rights under at least one of the first DRM and
11 the second DRM to the file.

12

13 13. The encoder according to claim 10, wherein the first and second pointers
14 comprise byte offsets identifying a starting location for encrypted segments of
15 content.

16

17 14. The encoder according to claim 10, wherein the first and second
18 encrypted segments of content have a duration defined by an encryption quanta.

19

20 15. The encoder according to claim 10, further comprising appending data to
21 enable digital rights under at least one of the first DRM and the second DRM to
22 the file; and transmitting the file to a customer.

23

24 16. The encoder according to claim 10, implemented in a programmed
25 general purpose computer.

26

- 1 17. A method of using rights to digital content under one of a plurality of digital
2 rights management scenarios (DRM), comprising:
3 carrying out a transaction to acquire digital rights to the content;
4 receiving digital content containing:
5 segments of unencrypted content,
6 first encrypted segments of content encrypted using a first
7 encryption method associated with a first DRM,
8 second encrypted segments of content encrypted using a second
9 encryption method associated with a second DRM,
10 first pointers to the first encrypted segments of content;
11 second pointers to the second encrypted segments of content, and
12 DRM data that enables digital rights under at least one of the first
13 DRM and the second DRM;
14 determining that valid digital rights are available from the DRM data; and
15 decrypting one of the first and second encrypted segments to enable
16 playing of the content.
17
- 18 18. The method according to claim 17, wherein the content comprises at least
19 one of digitized audio and digitized video.
20
- 21 19. The method according to claim 17, wherein the first and second pointers
22 comprise byte offsets identifying a starting location for encrypted segments of
23 content.
24
- 25 20. The method according to claim 17, wherein the first and second encrypted
26 segments of content have a duration defined by an encryption quanta.
27

- 1 21. A computer readable medium storing instructions which, when executed
2 on a programmed processor, carry out the method of method of using rights to
3 digital content according to claim 17.
- 4 22. A decoder that enables use rights to digital content under one of a plurality
5 of digital rights management scenarios (DRM), comprising:
6 means for carrying out a transaction to acquire digital rights to the content;
7 means for receiving digital content containing:
8 segments of unencrypted content,
9 first encrypted segments of content encrypted using a first
10 encryption method associated with a first DRM,
11 second encrypted segments of content encrypted using a second
12 encryption method associated with a second DRM,
13 first pointers to the first encrypted segments of content;
14 second pointers to the second encrypted segments of content, and
15 DRM data that enables digital rights under at least one of the first
16 DRM and the second DRM;
17 a DRM validator that determines that valid digital rights are available from
18 the DRM data; and
19 a decrypter that decrypts one of the encrypted segments to enable playing
20 the content.
21
- 22 23. The decrypter according to claim 22, wherein the content comprises at
23 least one of digitized audio and digitized video.
24
- 25 24. The decrypter according to claim 22, wherein the first and second pointers
26 comprise byte offsets identifying a starting location for encrypted segments of
27 content.
28

1 25. The decrypter according to claim 22, wherein the first and second
2 encrypted segments of content have a duration defined by an encryption quanta.

3

4 26. The decrypter according to claim 22, implemented in a programmed
5 general purpose computer.

6

7 27. A selectively encrypted digital content signal that enables use of multiple
8 digital rights management scenarios (DRM) embodied in a carrier wave,
9 comprising:

10 segments of unencrypted content;

11 first encrypted segments of content encrypted using a first
12 encryption method associated with a first DRM;

13 second encrypted segments of content encrypted using a second
14 encryption method associated with a second DRM;

15 a first segment of code comprising first pointers to the first
16 encrypted segments of content;

17 a second segment of code comprising second pointers to the
18 second encrypted segments of content; and

19 a segment of DRM data that enables digital rights under at least
20 one of the first DRM and the second DRM.

21

22 28. The carrier wave according to claim 27, wherein the content comprises at
23 least one of digitized audio and digitized video.

24

25 29. The carrier wave according to claim 27, wherein the first and second
26 pointers comprise byte offsets identifying a starting location for encrypted
27 segments of content.

28

1 30. The carrier wave according to claim 27, wherein the first and second
2 encrypted segments of content have a duration defined by an encryption quanta.
3

4 31. A selectively encrypted digital content signal that enables use of multiple
5 digital rights management scenarios (DRM) embodied in a computer
6 readable medium, comprising:

7 segments of unencrypted content;

8 first encrypted segments of content encrypted using a first
9 encryption method associated with a first DRM;

10 second encrypted segments of content encrypted using a second
11 encryption method associated with a second DRM;

12 a first segment of code comprising first pointers to the first
13 encrypted segments of content;

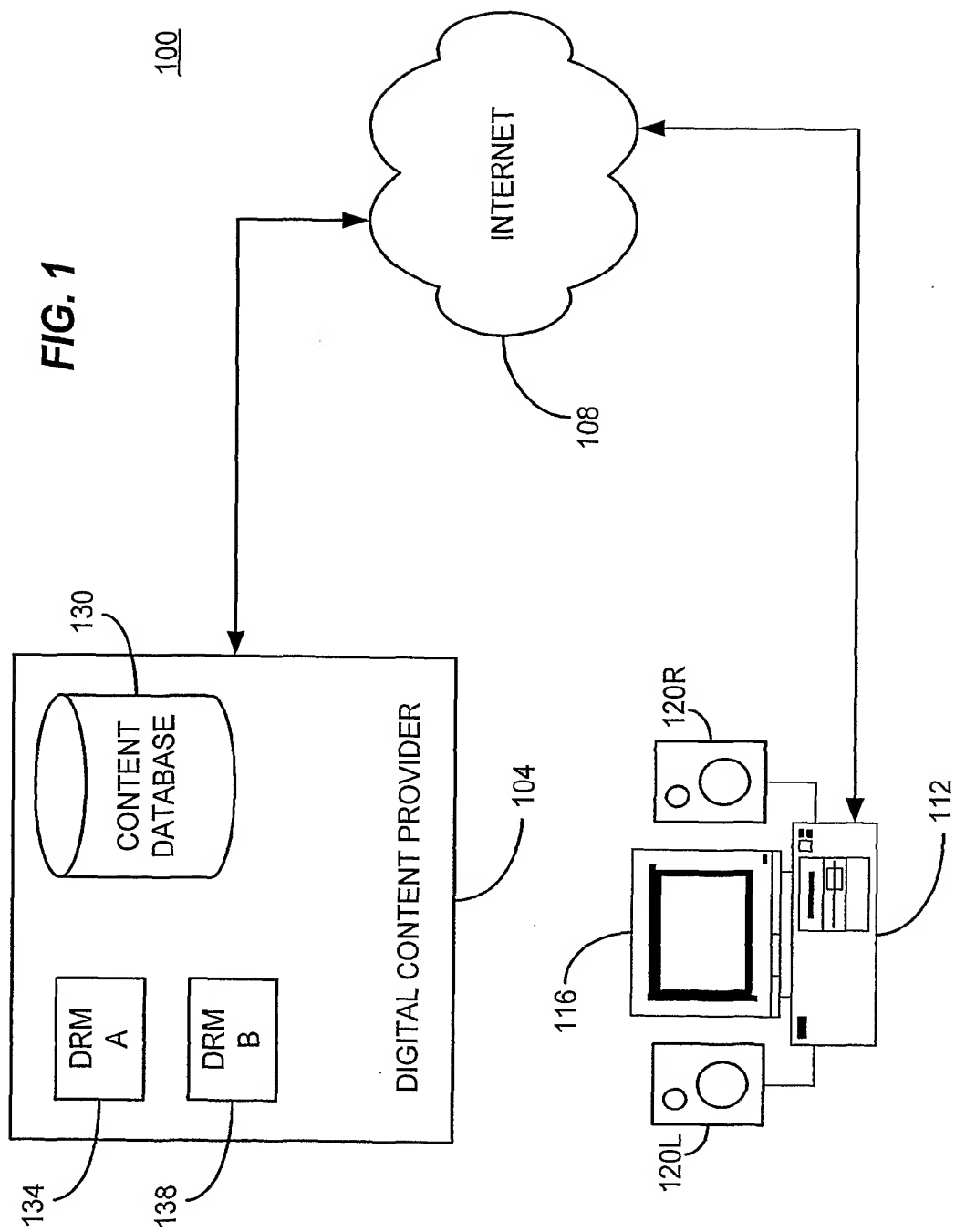
14 a second segment of code comprising second pointers to the
15 second encrypted segments of content; and

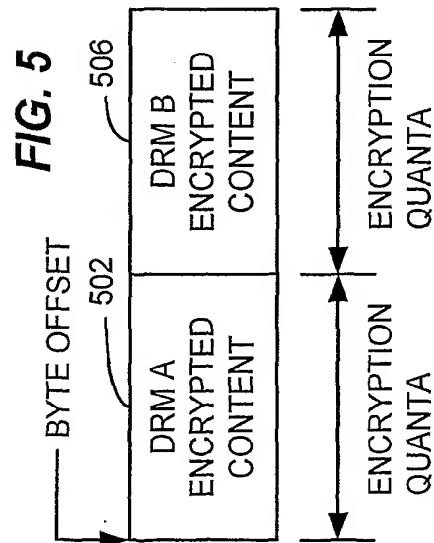
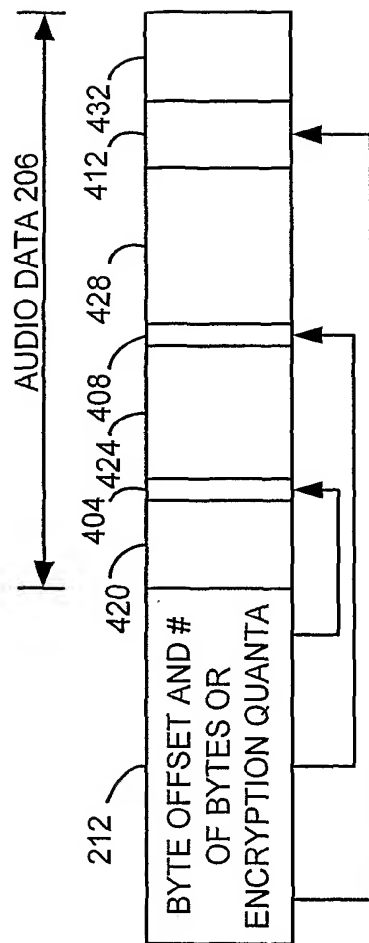
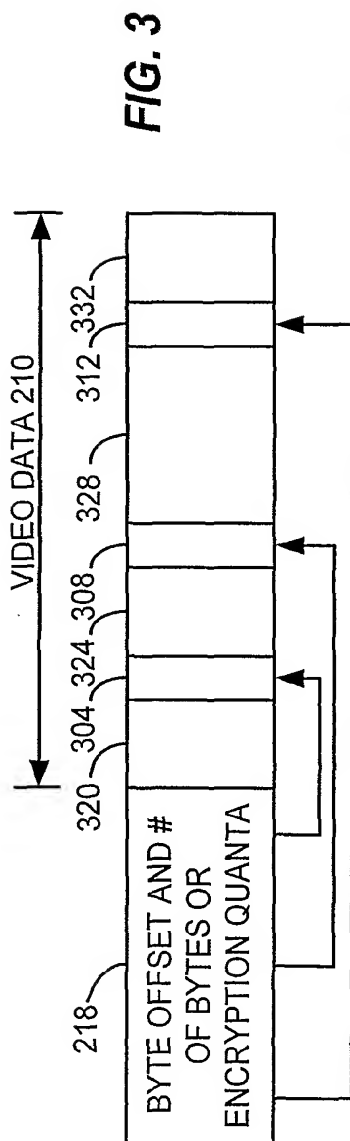
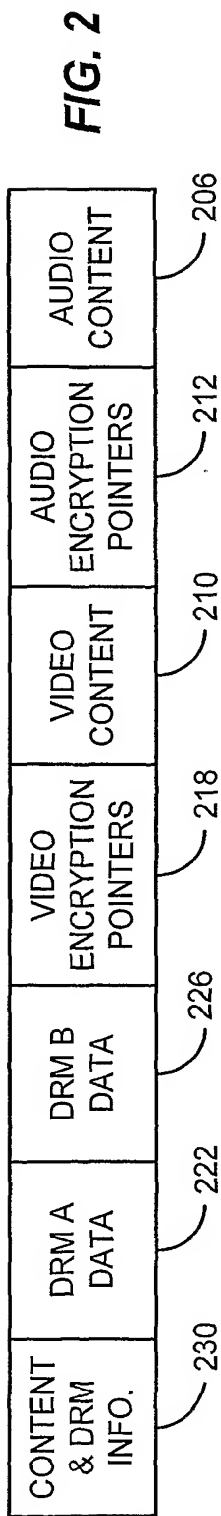
16 a segment of DRM data that enables digital rights under at least
17 one of the first DRM and the second DRM.
18

19 32. The computer readable medium according to claim 31, wherein the
20 content comprises at least one of digitized audio and digitized video.
21

22 33. The computer readable medium according to claim 31, wherein the first
23 and second pointers comprise byte offsets identifying a starting location for
24 encrypted segments of content.
25

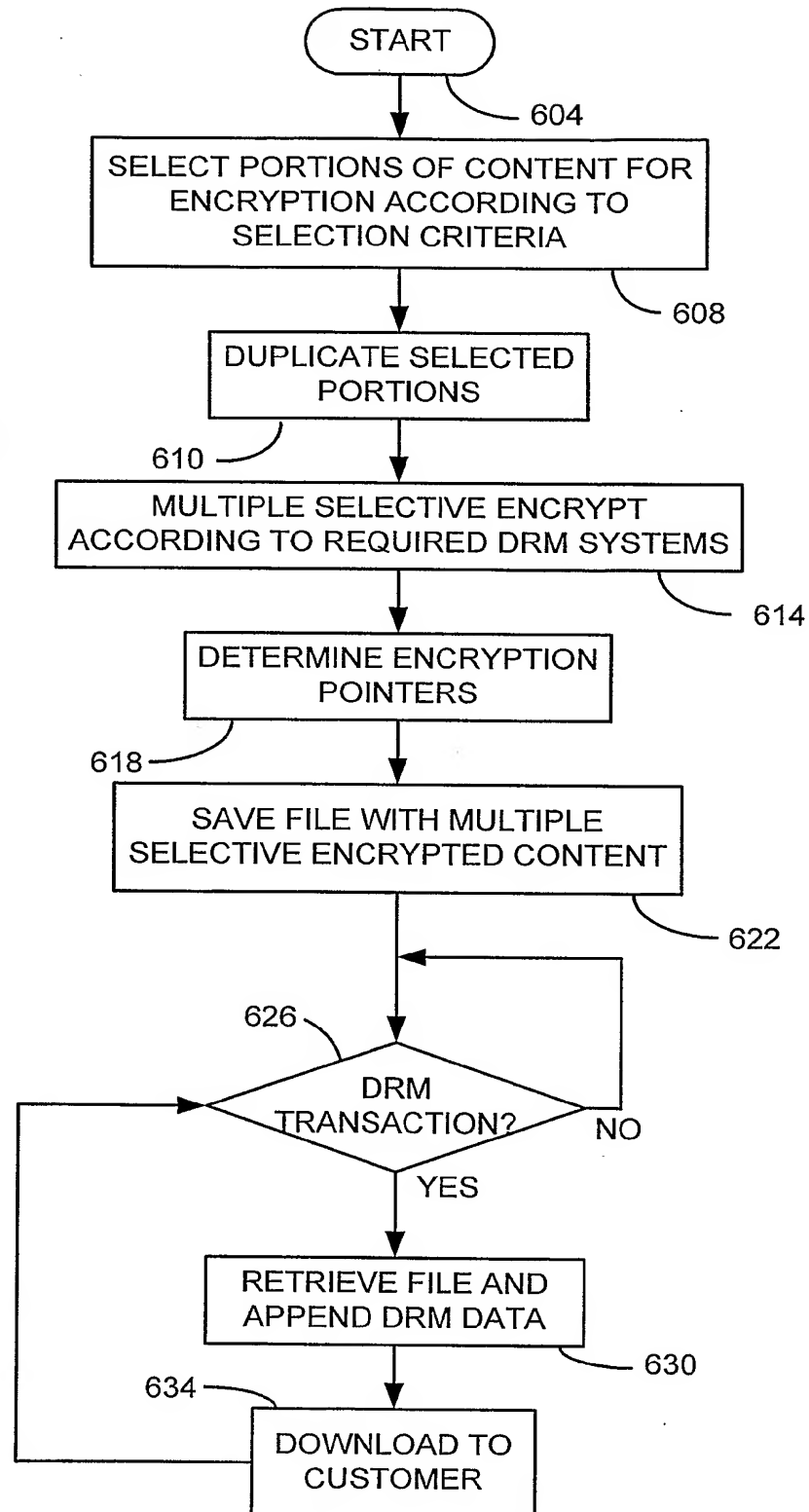
26 34. The computer readable medium according to claim 31, wherein the first
27 and second encrypted segments of content have a duration defined by an
28 encryption quanta.

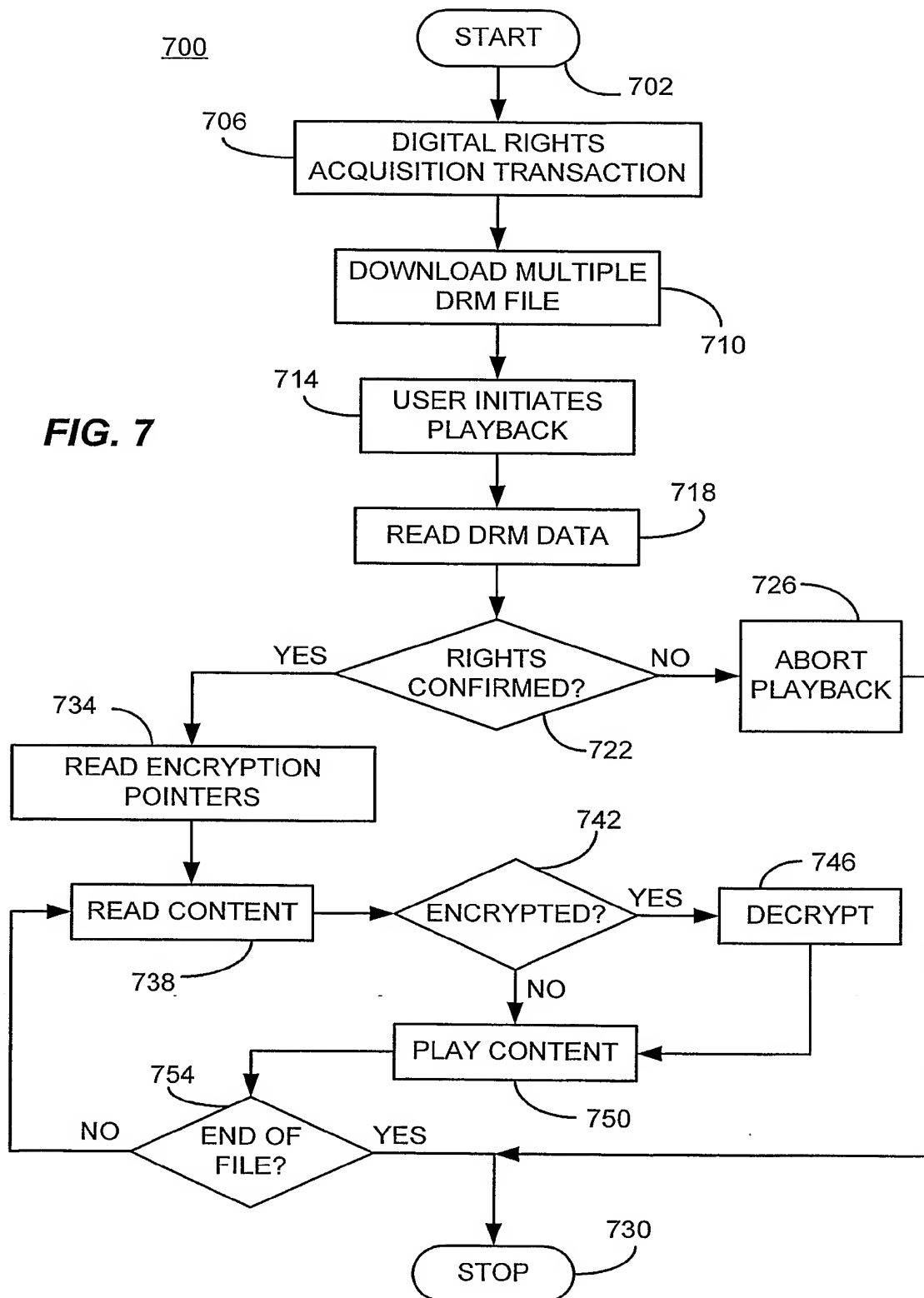
FIG. 1

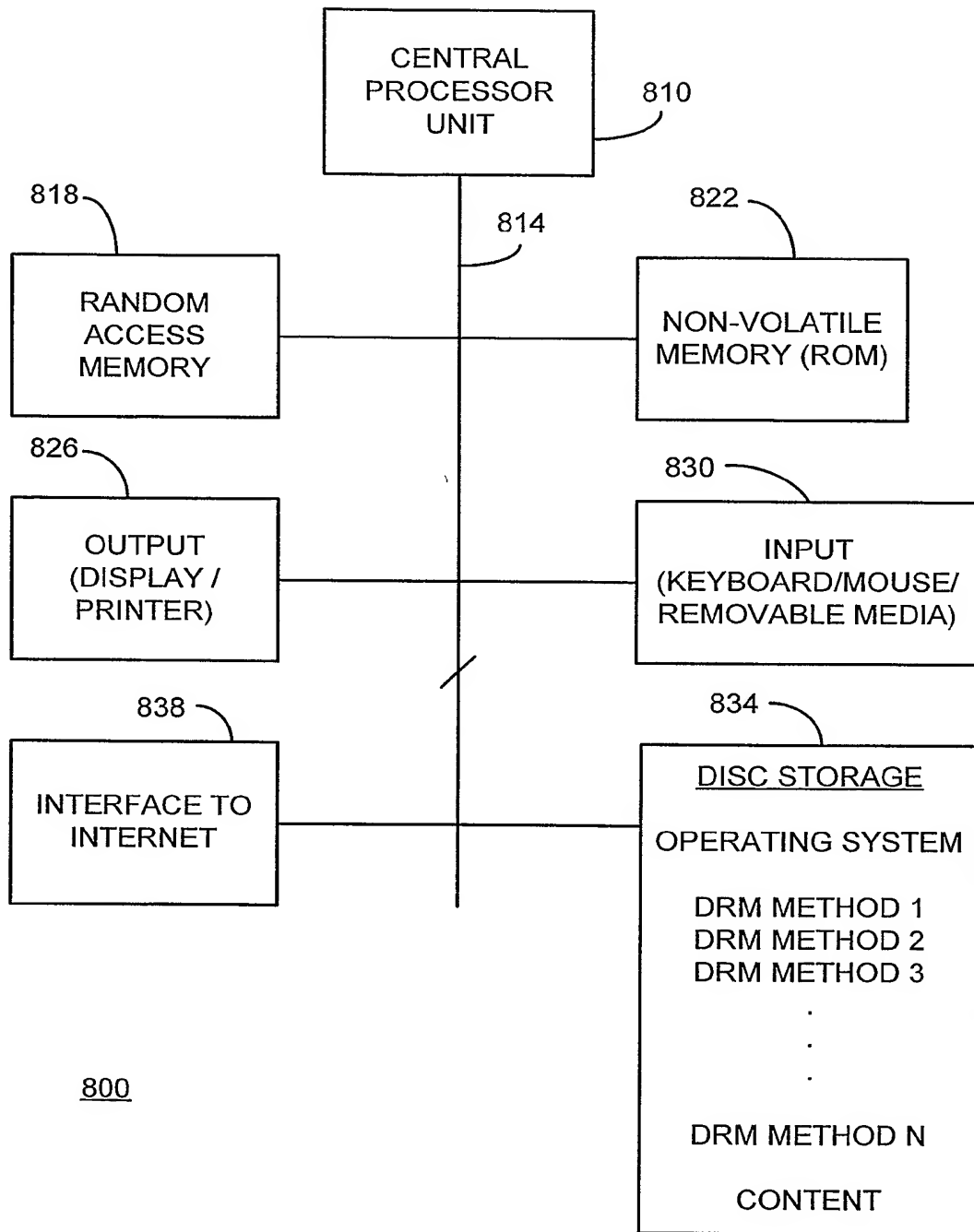


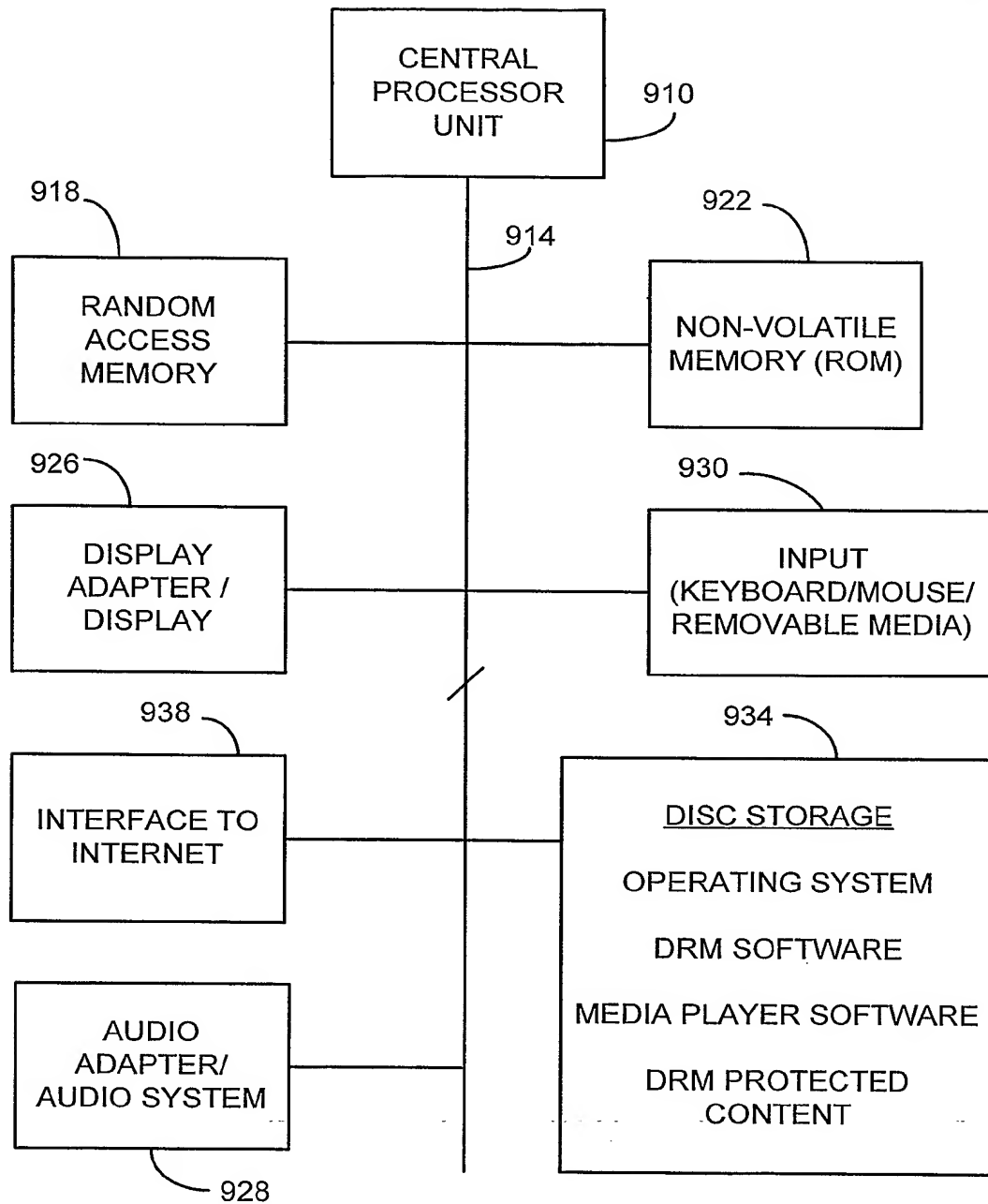
600

FIG. 6





**FIG. 8**

**FIG. 9**900